G.N. (E.) 74 of 2020

Operating Principles and Guidelines for Application for Authorization to Conduct Interception and Covert Surveillance

Issued Pursuant to Section 20 of Schedule 6 of the Implementation Rules for Article 43 of the Law of the People's Republic of China on Safeguarding National Security in the Hong Kong Special Administrative Region

A. **GENERAL** 1785

B. **CONDITIONS FOR ISSUE, RENEWAL OR CONTINUANCE OF PRESCRIBED AUTHORIZATION** 1785

C. **PRESCRIBED AUTHORIZATIONS** 1786

C1. Relevant Authorities 1786

D. **APPLICATION PROCEDURES** 1787

D1. General Rules 1787

D2. Chief Executive's authorization for interception or covert surveillance 1787

D3. Chief Executive's authorization for Type 2 surveillance 1789

D4. Emergency Authorization 1790

D5. Protection of Legal Professional Privilege information 1792

D6. Material inaccuracy or material change in circumstances 1793

	D7.	Care in implementation	1794
	D8.	Device Retrieval Warrant	1795
E.	**SUPERVISING RESPONSIBILITY**		1795
	E1.	Supervision by the National Security Committee	1795
	E2.	Regular Reviews by the Police Force	1796
	E3.	Safeguards for Protected Products	1796
F.	**RETENTION OF RECORDS**		1797
G.	**ENSURING COMPLIANCE**		1798

A. GENERAL

The Operating Principles and Guidelines are issued under Section 20 of the Rules on Application for Authorization to Conduct Interception and Covert Surveillance (Schedule 6 of the Implementation Rules for Article 43 of the Law of the People's Republic of China on Safeguarding National Security in the Hong Kong Special Administrative Region) to provide operating principles and guidance to officers of the Police Force. Officers of the Police Force have a duty to comply with the provisions of the Operating Principles and Guidelines in performing the functions under Schedule 6. If any officer fails to comply with the provisions of Schedule 6, the terms of the prescribed authorization or device retrieval warrant concerned, or the provisions of the Operating Principles and Guidelines, the Police Force should report to the Committee for Safeguarding National Security of the Hong Kong Special Administrative Region ("the National Security Committee").

2. Unless the context otherwise requires, the interpretation of terms used in the Operating Principles and Guidelines should follow that set out in Schedule 6.

B. CONDITIONS FOR ISSUE, RENEWAL OR CONTINUANCE OF PRESCRIBED AUTHORIZATION

3. Provisions in Chapter III of the Basic Law protect relevant rights and freedoms. The underlying principle is that any impact on any such rights and freedoms by the covert operations authorized and conducted under Schedule 6 must be necessary for and proportionate to the purposes that such operations seek to achieve.

4. Section 2 of Schedule 6 sets out the conditions for the issue, confirmation or renewal of a prescribed authorization, or the continuance of a prescribed authorization or a part of a prescribed authorization for interception of communications or covert surveillance. Covert operations authorised under Schedule 6 must be for the purpose of preventing or detecting national security offences or protecting national security. The person issuing the authorization

must have reasonable suspicion that any person has been, is, or is likely to be, involved in national security offences or activities which constitute threats to national security. The authorizing authority must consider the immediacy and gravity of the case, and whether other less intrusive means can be reasonably adopted.

5. An application for interception or covert surveillance which is likely to result in the acquisition of information which may be subject to legal professional privilege (LPP) should only be made in exceptional circumstances with full justifications. Particular attention should be given to that factor in considering whether such operation is proportionate to the purpose. The application must include an assessment of how likely it is that such privileged information will be obtained. For more details about the measures that should be put in place to protect such privileged information, see the part on "Protection of Legal Professional Privilege Information" in paragraphs 23 to 25 below.

C. PRESCRIBED AUTHORIZATIONS

C1. Relevant Authorities

6. The "relevant authority" for considering applications for prescribed authorizations is as follows:—

(a) Interception and Type 1 Surveillance

- The Chief Executive.

(b) Type 2 Surveillance

- The Chief Executive; or
- An authorizing officer designated by the Chief Executive whose substantive rank is not below the rank of chief superintendent of police,

as may be applicable.

(c) Emergency Authorization

- The Commissioner of Police (subsequent confirmation by the Chief Executive is required).

7. When an authorizing officer considers whether to issue an authorization for Type 2 surveillance, in no case should:—

(a) the authorizing officer be directly involved in the investigation of the case covered by the application for authorization;

(b) the applying officer be the same person as the authorizing officer; or

(c) the authorizing officer be involved in formulating the application.

D. APPLICATION PROCEDURES

D1. GENERAL RULES

8. The applicant for applications to be made under Schedule 6 should be a police officer who is responsible for the enforcement of the Law of the People's Republic of China on Safeguarding National Security in the Hong Kong Special Administrative Region ("National Security Law") and should not be lower in rank than inspector of police. The applicant should also be conversant with the facts of the case.

D2. CHIEF EXECUTIVE'S AUTHORIZATION FOR INTERCEPTION OR COVERT SURVEILLANCE

9. This part applies to applications for the issue or renewal of a prescribed authorization for carrying out interception of communications, Type 1 surveillance or Type 2 surveillance, in accordance with Division 1 of Part 2 of Schedule 6. Upon obtaining an approval from a directorate officer of the Police Force, an officer of the Police Force may apply to the Chief Executive for the issue of a Chief Executive's authorization for interception, Type 1 surveillance or Type 2 surveillance. The application for a Chief Executive's authorization for interception, Type 1 surveillance or Type 2 surveillance shall be made in writing and supported by a statement in writing made by the applicant detailing the facts which are relied upon to obtain the authorization. The statement should include the relevant

information specified in Division 1 or 2 of Part 4 of Schedule 6 (as may be applicable). The Chief Executive will communicate the determination in writing.

10. If a Chief Executive's authorization in force has to be renewed, a renewal application must be made before the authorization ceases to have effect. The renewal will take effect at the time when the Chief Executive's authorization would have ceased to have effect but for the renewal, i.e. the time of expiry of the authorization sought to be renewed. A Chief Executive's authorization may be renewed more than once. The Chief Executive will communicate the determination in writing.

Authorization for Type 2 surveillance considered as a Type 1 surveillance

11. Where there is a likelihood of a Type 2 surveillance operation obtaining information which may be subject to LPP, the Type 2 surveillance is regarded as Type 1 surveillance under section 27(3) of Schedule 6. In these circumstances, the Police Force must apply to the Chief Executive for a prescribed authorization for Type 1 surveillance even though the covert surveillance is otherwise Type 2 surveillance. On the other hand, section 27(4) of Schedule 6 provides that an officer may apply for the issue or renewal of a prescribed authorization for Type 2 surveillance as if the Type 2 surveillance were Type 1 surveillance, and the provisions of Schedule 6 relating to the application and the prescribed authorization apply to the Type 2 surveillance as if it were Type 1 surveillance. Officers should consider making an application to the Chief Executive if the operation would involve both Type 1 and Type 2 surveillance, thus obviating the need to apply to both the Chief Executive and an authorizing officer for all the authorisations required for the same operation.

12. In addition, there exists special circumstances which may render a Type 2 surveillance operation particularly intrusive, for example:—

- there is a likelihood that contents of journalistic material may be obtained; or

- an electronic optical surveillance device is proposed to be directed at a person inside premises from outside those premises in circumstances where the person has taken measures to protect his privacy such that, were it not for the use of that device, he would not be observable by a person outside the premises.

In such situations, consideration should be given by the Police Force for applying to the Chief Executive instead of an authorizing officer for a prescribed authorization for Type 2 surveillance under section 27(4) of Schedule 6.

D3. Chief Executive's authorization for Type 2 surveillance

13. This part applies to applications for issue or renewal of an authorization for Type 2 surveillance in compliance with Division 1 of Part 2 of Schedule 6. The relevant authority for considering such applications is the Chief Executive, or an authorizing officer designated by the Chief Executive whose substantive rank is not below the rank of chief superintendent of police. The application for a Chief Executive's authorization for Type 2 surveillance shall be made in writing and supported by a statement in writing made by the applicant detailing the facts which are relied upon to obtain the authorization. The statement should include the relevant information specified in Division 2 of Part 4 of Schedule 6. The Chief Executive or an authorizing officer (as may be applicable) will communicate the determination in writing.

14. The Chief Executive or an authorizing officer (as may be applicable) should take a critical approach when considering applications, including whether the application is fully justified and whether the duration sought is reasonable. The authorizing officer should not approve an application as a matter of course or consider the application solely in light of his knowledge of the case in question. Where necessary, he should seek clarification and explanation from the applicant before he comes to any determination.

15. In considering an application, the Chief Executive or an authorizing officer (as may be applicable) must be satisfied that the conditions for issuing the authorization set out in section 2 of Schedule 6 (see paragraph 4 above) are all met. The particular intrusiveness of the operation because of the nature of the information that may be obtained (such as journalistic material), the identity of the subject (such as lawyers or paralegals), etc. may be relevant (paragraph 12 above). In particular, special attention should be paid to the assessment of the likelihood that information which may be subject to LPP will be obtained. If an authorizing officer considers that LPP information is likely to be obtained through the proposed covert surveillance operation, he should refuse the application for Type 2 surveillance and direct the applicant to make an application to the Chief Executive for authorization for Type 1 surveillance (paragraph 11 above).

D4. EMERGENCY AUTHORIZATION

16. This part applies to applications for emergency authorizations for carrying out interception of communications or Type 1 surveillance under Division 2 of Part 2 of Schedule 6. The Commissioner of Police is authorized to issue emergency authorizations under specified circumstances.

17. Section 9 of Schedule 6 provides that an officer of the Police Force may apply to the Commissioner of Police for the issue of an emergency authorization for interception or Type 1 surveillance under specified circumstances. It refers to, inter alia, the terms "imminent risk", "substantial damage" and "vital evidence". What constitutes such risk, damage or evidence depends much on the circumstances of each case. In general terms, an "imminent" risk is a very near and impending risk. "Substantial" damage is damage which is large in amount, or extent. "Vital" evidence is evidence which is necessary or very important in supporting a case. The applicant should be satisfied that the gravity of the case justifies the issue of the emergency authorization.

18. Officers of the Police Force are reminded that an application for emergency authorization should only be made if it is not reasonably

practicable in the circumstances to apply for a Chief Executive's authorization in writing. It should only be used as a last resort. A Chief Executive's authorization should be applied for whenever it is reasonably practicable to do so.

19. The Commissioner of Police shall not issue the emergency authorization unless he is satisfied that the emergency conditions (see paragraph 17) and the conditions for issuing the authorization set out in section 2 of Schedule 6 (see paragraph 4 above) are all met.

20. Schedule 6 provides that where any interception or Type 1 surveillance is carried out pursuant to an emergency authorization, the Commissioner of Police shall cause an officer of the Police Force to apply to the Chief Executive for confirmation of the emergency authorization as soon as reasonably practicable, and in any event within the period of 48 hours beginning with the time when the emergency authorization is issued, irrespective of whether the interception / covert surveillance has been completed or not. The application for confirmation should be made by the same officer who has applied for the emergency authorization as far as practicable.

21. It is essential that application for confirmation of an authorization be made within 48 hours of the issue of the emergency authorization. To ensure close attention is paid to the situation of the emergency authorization, the Commissioner of Police should put in place arrangements for emergency authorizations to be closely tracked, and that his personal attention be brought to any failure to comply with the requirement to apply for confirmation within 48 hours. Any failure to apply for confirmation of an emergency authorization is a non-compliance for which the National Security Committee should be notified as soon as practicable, followed by a full report. Section 10(2) of Schedule 6 provides that in default of any application being made for confirmation of the emergency authorization within the 48 hours, the Commissioner of Police shall cause the immediate destruction of any information obtained by carrying out the interception or Type 1 surveillance. In this connection, "information" includes all products as well as any other information obtained by carrying out the interception / covert surveillance.

Special Procedures for Emergency Authorizations applied for and issued orally

22. Under exceptional circumstances, an application for the issue of an emergency authorization may be made orally, if the applicant considers that it is not reasonably practicable, having regard to all the circumstances of the case, to make the application in writing. The Commissioner of Police may also issue emergency authorization orally under exceptional circumstances. The applicant should record in writing the relevant application and authorization as soon as practicable, and in any event before the application for confirmation of the authorization.

D5. Protection of Legal Professional Privilege information

23. As with all other law enforcement actions, the Police Force shall in no case knowingly seek to obtain information subject to LPP in undertaking covert operations authorized under Schedule 6. Indeed, Schedule 6 seeks to minimize the risk of inadvertently obtaining information that may be subject to LPP during such operations. Section 13 of Schedule 6 prohibits the carrying out of interception or covert surveillance in a lawyer's office, residence and other relevant premises in the circumstances described in that section unless exceptional circumstances exist. Examples of relevant premises include interview rooms of courts, prisons, police stations and other places of detention where lawyers regularly provide legal advice to their clients.

24. Officers should therefore take extreme care when approaching possible applications that concern the premises and / or telecommunications services used by a lawyer. A risk assessment must be conducted if the interception or covert surveillance may acquire information that may be subject to LPP. In this connection, officers are reminded that LPP is not lost if a lawyer is properly advising a person who is suspected of having committed a criminal offence. Unless they are fully satisfied that the exceptional circumstances under section 13(2) of Schedule 6 exist, officers should not make an application for an authorization targeting these premises and telecommunications services. In all such exceptional cases, an

authorization issued personally by the Chief Executive must be obtained even if the operation sought to be carried out would otherwise be a Type 2 surveillance operation under normal circumstances, and justification for the proposed interception / covert surveillance should be given in the statement supporting the application.

25. Any information that is subject to LPP will remain privileged notwithstanding that it has been inadvertently obtained pursuant to a prescribed authorization. Dedicated units separate from the investigation team shall screen out information protected by LPP, and to withhold such information from the investigators. The only possible exception to this arrangement of initial screening by separate dedicated units is covert surveillance involving participant monitoring where, for the safety or well-being of the participants participating in the conversation (including the victims of crimes under investigation, informers or undercover officers), or in situations that may call for the taking of immediate arrest action, there may be a need for the investigators to listen to the conversations in real time. In such circumstances, it will be specified in the application to the relevant authority, who will take this into account in deciding whether to issue an authorization and, if so, whether any conditions should be imposed. After such an operation, investigators monitoring the operations will be required to hand over the recording to the dedicated units, who will screen out any information subject to LPP before passing it to the investigators for their retention.

D6. Material inaccuracy or material change in circumstances

26. Under section 18 of Schedule 6, where the officer in charge of the interception or covert surveillance becomes aware that there is a material inaccuracy in the information provided for the purposes of the application for the issue or renewal of a prescribed authorization (or confirmation of an emergency authorization), or there is a material change in the circumstances on the basis of which the authorization was issued or renewed (or the emergency authorization was confirmed), he must cause a report on the material inaccuracy or material change in circumstances to be provided to the relevant

authority as soon as reasonably practicable after becoming aware of the matter. On receiving the report, the relevant authority will revoke the authorization or a part of the authorization if he considers that the conditions for the continuance of the authorization or that part of the authorization are not met. A copy of the report with the determination of the relevant authority should be provided to the National Security Committee. Examples of "material inaccuracy" and "material change in circumstances" are as follows:—

Material inaccuracy	• Incorrect information in relation to the particulars of the subject • Incorrect information in relation to the background of application or case details
Material change in circumstances	• Heightened likelihood of obtaining information subject to LPP or journalistic material • New information on the identity of the subject uncovered during operation • New information relevant to the determination of an application for the issue or renewal of an authorization • Arrest of the subject

D7. Care in implementation

27. Reasonable force, as authorized, should only be used if it is necessary for carrying out an authorization and should be kept to the minimum required. The same minimization principle applies to any interference with property. While an authorization authorizes interference with property, this is limited to the extent incidental to and necessary for the implementation of the authorization. Officers should at all times ensure that such interference and any damage that might be caused to property is kept to the absolute minimum. In the event that any unavoidable damage is caused to property, all efforts must be made to make good the damage. Where parties whose property has been interfered claim for damages, the Police Force

should handle the claims in the same manner as other cases arising from any law enforcement operations.

D8. Device Retrieval Warrant

28. As a matter of policy, surveillance devices should not be left in the target premises after the completion or discontinuance of the covert surveillance operation, in order to protect the privacy of the individuals affected and the covert nature of the operation. An authorization already authorizes the retrieval of a surveillance device within the period of authorization, and surveillance devices should be retrieved during the period of authorization. As a general rule, after the expiry of the authorization, unless it is not reasonably practicable to retrieve the device, an application must be made for a device retrieval warrant if the device has not yet been retrieved. In all cases, at the expiration of the authorization, the officer-in-charge of the covert surveillance operation should take all reasonably practicable steps as soon as possible to deactivate the device, or to withdraw any equipment that is capable of receiving signals or data that may still be transmitted by a device if it cannot be deactivated.

E. SUPERVISING RESPONSIBILITY

E1. Supervision by the National Security Committee

29. According to paragraph 2 of Article 43 of the National Security Law, the National Security Committee shall be responsible for supervising the implementation of measures stipulated in paragraph 1 of that Article by law enforcement authorities including the department for safeguarding national security of the Police Force. This includes carrying out interception of communications and conducting covert surveillance on a person who is suspected, on reasonable grounds, of having involved in the commission of an offence endangering national security upon approval of the Chief Executive (see item 6 of paragraph 1 of Article 43 of the National Security Law). Section 19 of Schedule 6 stipulates that the Chief Executive may appoint an independent person to assist the National

Security Committee in performing its supervising responsibilities under Article 43 of the National Security Law.

E2. Regular Reviews by the Police Force

30. The Commissioner of Police shall make arrangements to keep under regular review the compliance by officers of the Police Force with the provisions of Schedule 6, the terms of the prescribed authorization or device retrieval warrant concerned, and the provisions of the Operating Principles and Guidelines. The regular reviews will be conducted by an officer not below the rank of Assistant Commissioner of Police. The reviews may consist of audit checks of past and live cases as well as theme-based targeted reviews. The reviewing officer should, as far as practicable, be an officer who is or was not directly involved in the investigation or operation in question.

31. If any instance of non-compliance (whether or not due to the fault of the Police Force or any of its officers) with the above requirements is identified during such reviews or an officer of the Police Force is otherwise made aware of it, arrangements should be in place for notifying the non-compliance to the National Security Committee as soon as practicable, followed by a full report.

E3. Safeguards for Protected Products

32. Where any protected product[1] has been obtained pursuant to any prescribed authorization, the Commissioner of Police should make arrangements to ensure that the requirements in section 16 of Schedule 6 are satisfied.

33. The Commissioner of Police should ensure that any part of the protected product that contains information subject to LPP:—

(a) in the case of an authorization for a postal interception or covert surveillance, is destroyed not later than 1 year after its retention ceases to be necessary for civil or criminal

1 Copies of protected products are subject to the same protection requirements as those for the products themselves under the Ordinance. "Copy" is defined to include any copy, extract or summary of the contents.

proceedings before any court that are pending or are likely to be instituted; or

(b) in the case of an authorization for a telecommunications interception, is as soon as reasonably practicable destroyed.

In no case should any such LPP information be used for any other purposes.

34. To protect privacy and ensure the integrity of these covert operations, details of each operation should only be made known on a strict "need to know" basis.

35. Schedule 6 provides that any relevant telecommunications interception product is not admissible in evidence in any proceedings before any court other than to prove that a "relevant offence" constituted by the disclosure of a telecommunications interception product or of information relating to the obtaining of a telecommunications interception product.

F. RETENTION OF RECORDS

36. The Police Force should, on the basis of their mode of operation, set up system(s) to document the information obtained from interception / covert surveillance authorized under Schedule 6, with restricted access to the different types of information depending on the confidentiality level, and keep a proper paper trail on access, disclosure and reproduction. The Police Force should maintain a central registry to keep the records associated with applications for prescribed authorizations and related matters.

37. The Police Force should also ensure that proper records with clear description of the exact usage are kept on the inventories and movement of devices to minimize the possibility of unauthorized usage. Moreover, to minimize the chance of possible abuse in the use of the devices by frontline officers for unauthorized purposes, only in

justified circumstances should officers of the Police Force be allowed to keep the surveillance devices.

38. To protect the confidentiality of the information kept, it is essential that strict access control be implemented. The established requirements for physical security protection, access control and "need to know" principle should be complied with.

G. ENSURING COMPLIANCE

39. Officers who fail to comply with the provisions of Schedule 6, the terms of the prescribed authorization or device retrieval warrant concerned, or the provisions of the Operating Principles and Guidelines would be subject to disciplinary action or, depending on the case, the common law offence of misconduct in public office, in addition to continuing to be subject to the full range of existing law. The Police Force should therefore ensure that officers who may be involved in the application for, or determination of and execution of matters covered by Schedule 6 are fully briefed on the various requirements. Refresher briefings should be arranged as and when the Operating Principles and Guidelines is updated or after important recommendations or directives of reference value are made by the National Security Committee or the reviewing officer that may be of general reference value.

40. The Operating Principles and Guidelines, and future revisions thereof, will be gazetted for general information.

July 2020 *Secretary for Security*